Cryptography in the Quantum World

Claude Crépeau*

School of Computer Science, McGill University, Montréal (Québec), Canada, e-mail: crepeau@cs.mcgill.ca

Classical information deals with discrete finite alphabets such as $\{0,1\}$ used for binary representation. On the other hand, Quantum information offers a wider range of possibilities: any linear combinaison $\alpha|0\rangle + \beta|1\rangle$, where $|0\rangle, |1\rangle$ are two orthogonal states of a quantum system and where α, β are any complex numbers such that $||\alpha||^2 + ||\beta||^2 = 1$, are possible values of a *qubit* (quantum bit).

A quantum computer, i.e. a machine that computes with qubits, is different from a simple *analog* machine because quantum information follows special rules described by quantum physics[8]: quantum information cannot be copied or broadcast and cannot be read accurately. Only certain kinds of measurements are possible[8]. The computing power of a quantum machine is not only due to the extended range of values but also to the evolution rules due to quantum physics. It turns out that difficult computations such as *factoring large numbers* and *extracting discrete logarithms* appear to be faster on a quantum computer [10] than on a classical computer.

We survey a number of results concerning transmission of quantum information secretly. First of all, we present the basic concepts of quantum information and the rules guiding it. Then we consider *quantum teleportation*[3] which is the quantum equivalent of the classical *one-time-pad*, showing the possibility of transmission of perfectly secret quantum messages as long as the users have exchanged a (quantum) secret key before end of a special Einstein-Podolsky-Rosen type.

Then we consider *quantum cryptography*[1, 2, 7], a technique used to secretly exchange a cryptographic key using the uncertainty principle to determine the amount of tempering on the communication. We unveil a technique known as *entanglement purification*[5] that publicly allows amplification of the privacy [4] of a random secret key. Combined with quantum cryptography this technique allows users to exchange EPR particles publicly and purify them after tempering of an adversary in order to transmit secret information through teleportation.

Finally, the quantum equivalent[6] of Shamir's secret sharing[9] is presented. A $((n,k))$ quantum threshold scheme is a technique that allows to break a quantum secret s into *shares* $s_1, s_2, \ldots, s_n$ such that any subset of up to $k-1$ such shares contain no information about s, while any subset of k such shares can be used to recover exactly s. The existence of such a scheme is strongly connected to the existence of certain types of quantum error-correcting codes[11, 12].

References

[1] Bennett, C. H. and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175–179, Dec 1984.

[2] Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, Experimental quantum cryptography, *Journal of Cryptology*, Vol. 5, no. 1, 3–28, 1992.

[3] Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. Wootters, Teleporting an unknown quantum state by dual classical and EPR channels. *Physical Review Letter*, 70:1895–1898, 1993.

[4] Bennett, C. H., G. Brassard, C. Crépeau and U. M. Maurer, Generalized privacy amplification, *IEEE Transaction on Information Theory*, Vol. 41, no. 6, November 1995, pp. 1915 – 1923.

[5] Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, *Physical Review Letter*, 76:722–725, Jan 1996.

[6] Cleve, R., D. Gottesman and H. K. Lo, How to share a quantum secret, *Los Alamos Quant-ph archive*, 9901025, 1999.

[7] Ekert, A. K., Quantum cryptography based on Bell's theorem, *Physical Review Letters*, Vol. 67, no. 6, 5 August 1991, pp. 661–663.

[8] Peres, A., *Quantum Theory: Concepts and Methods*, Fundamental Theories of Physics, Vol. 57, Kluwer Academic Publisher, 1993.

[9] Shamir, A., How to share a secret, *Communcations of the ACM*, 22:612–613, November 1979.

[10] Shor, P. W., Algorithms for quantum computation: Discrete log and factoring, *Proc. 35th IEEE Symposium on Foundations of Computer Science (FOCS)*, 124–134, 1994.

[11] Shor, P. W., Scheme for reducing decoherence in quantum memory, *Physical Review A*, Vol. 52, pp. 2493–2496, 1995.

[12] Steane, A. M., Error correcting codes in quantum theory, *Physical Review Letters*, Vol. 77, pp. 793–797, 1996.

* Supported in part by Canada's NSERC and Québec's FCAR.